CLAIMS

1   1.   A method for securely communicating information, said method comprising:

2   communicating an address to a first network device via the Internet such that the

3   first network device provides information corresponding to the address for use by a

4   second network device;

5   receiving encrypted information from the first network device via the Internet;

6   enabling the encrypted information to be posted at the address; and

7   enabling the second network device to access the address and retrieve the

8   encrypted information posted at the address.

1   2.   The method of claim 1, further comprising:

2   after the encrypted information has been retrieved by the second network device,

3   preventing the encrypted information from being retrieved from the address again.

1   3.   The method of claim 2, wherein a first firewall is communicatively coupled

2   between the first network device and the Internet.

1 4.   The method of claim 2, wherein the address provided to the first network device

2 is a first Uniform Resource Locator (URL) configured for a one-time use; and

3   wherein the second network device retrieves the encrypted information using a

4 second URL, the second URL being configured for a one-time use.

1 5.   The method of claim 1, wherein the encrypted information is provided from the

2 first network device to the second network device without either of the first and second

3 network devices being identified to the other.

1 6.   The method of claim 1, wherein the address is provided to the second network

2 device via a mobile appliance, the mobile appliance communicating with the first and

3 second network devices via wireless communication links.

1 7.   The method of claim 1, wherein a decryption key is provided to the second

2 network device via a secure communication protocol, the decryption key being

3 configured to enable decryption of the encrypted information.

1 8.   The method of claim 7, wherein the secure communication protocol uses the

2 Bluetooth specification.

1 9.   The method of claim 7, wherein the decryption key is provided to the second

2 network device via a mobile appliance, the mobile appliance communicating with the

3 first and second network devices via wireless communication links.

1   10.   The method of claim 9, wherein the decryption key is generated by the first

2   network device; and

3   wherein the mobile appliance receives the decryption key from the first network

4   device.

1   11.   The method of claim 1, wherein the second network device is a printing device

2   configured to receive the encrypted information, decrypt the information, and print the

3   information.

1   12.   A system for enabling secure communication of information between a first

2   network device and a second network device via the Internet, said system comprising:

3   a secure tunnel system communicating with the Internet;

4   the secure tunnel system being configured to:

5   provide address information to a first network device via the Internet;

6   receive encrypted information from the first network device via the

7   Internet,

8   post the encrypted information at an address associated with the address

9   information; and

10   enable a second network device to access and retrieve the encrypted

11   information from the address via the Internet while the encrypted information is

12   posted.

1   13.   The system of claim 12, wherein the secure tunnel system is configured to prevent

2   the encrypted information from being retrieved again after the encrypted information has

3   been retrieved by the second network device.

1   14.   The system of claim 12, further comprising:

2   means for preventing the encrypted information from being retrieved again after

3   the encrypted information has been retrieved by the second network device.

1   15.   The system of claim 14, wherein the means for preventing the encrypted

2   information from being retrieved again comprises:

3   means for generating a Uniform Resource Locator (URL) for use by the second

4   network device, the URL being configured for a one-time use such that, after the second

5   network device uses the URL to retrieve the encrypted information, the URL can no

6   longer be used to retrieve the encrypted information.

1   16.   A method for securely communicating information, said method comprising:

2   providing a first network device;

3   receiving, at the first network device, an address via the Internet;

4   providing a decryption key and the address to a mobile appliance via a secure

5 communication link; and

6   providing encrypted information to the address via the Internet, such that a second

7 network device is enabled to access and retrieve the encrypted information from the

8 address via the Internet while the encrypted information is posted and decrypt the

9 information using the decryption key provided from the mobile appliance.

1   17.   The method of claim 16, further comprising:

2   receiving an input from a user, the input corresponding to the user's intent to have

3   information communicated to the second network device;

4   in response to the user input, establishing communication with a third network

5   device via the Internet, the third network device being configured to provide the first

6   network device with a first Uniform Resource Locator (URL) for use by the first network

7   device and a second URL for use by the second network device, the first URL being

8   configured for a one-time use such that the first network device can post encrypted

9   information at the address using the first URL, the second URL being configured for a

10 one-time use such that the second network device can retrieve the encrypted information

11 from the address using the first URL; and

12   receiving the first and second URL's from the third network device.

1   18.   The method of claim 16, further comprising:

2   generating a decryption key for decrypting the encrypted information.

1   19.   A system for enabling secure communication of information between a first

2   network device and a second network device, said system comprising:

3   an information request system configured to communicate with the first and

4   second network devices,

5   the information request system being configured to receive an input from a user,

6   the input corresponding to the user's intent to have encrypted information communicated

7   to the second network device,

8   the information request system being further configured to receive a decryption

9   key and information corresponding to an address from the first network device in a secure

10   format, the information request system providing the decryption key and the information

11   corresponding to the address to the second network device in the secure format, thereby

12   enabling the second network device to access and retrieve encrypted information posted

13   on the Internet at the address and decrypt the information using the decryption key.

1   20.   The system of claim 19, further comprising:

2   a mobile appliance configured to communicate with the first and second network

3   devices; and

4   wherein the information request system is a part of the mobile appliance.